Table of Contents

# 1 Technical Architecture and Infrastructure Requirements

## 1.1 Introduction

This document outlines the technical architecture and infrastructure requirements for the Signox LogX System deployment across different scales and complexity levels.

## 1.2 System Architecture Overview

### 1.2.1 Core System Components

#### 1.2.1.1 Backend Services

* **Django REST API Backend**
  + Python 3.9+ with Django 4.2+
  + PostgreSQL 15+ database
  + Redis cache layer
  + Celery task queue
  + RESTful API endpoints

#### 1.2.1.2 Frontend Applications

* **Next.js Web Application**
  + TypeScript-based React application
  + Server-side rendering (SSR)
  + Progressive Web App (PWA) capabilities
  + Responsive design for all devices

#### 1.2.1.3 Supporting Services

* **Nginx Load Balancer**
  + SSL/TLS termination
  + Load balancing and failover
  + Static file serving
  + Request routing

### 1.2.2 Data Architecture

#### 1.2.2.1 Primary Database (PostgreSQL)

* **User Management**: Authentication, profiles, roles
* **Academic Structure**: Departments, programs, courses
* **Timetable Management**: Schedules, rooms, allocations
* **Attendance Records**: Sessions, check-ins, statistics
* **System Configuration**: Settings, rules, policies

#### 1.2.2.2 Cache Layer (Redis)

* Session storage
* Frequently accessed data
* Real-time notifications
* Task queue management

#### 1.2.2.3 File Storage

* User profile images
* Facial recognition data
* System backups
* Generated reports

## 1.3 Infrastructure Requirements by Scale

### 1.3.1 Small Institution (< 1,000 Users)

#### 1.3.1.1 Cloud-Based Deployment (Recommended)

**Application Infrastructure:** - **Web Application**: 2 CPU cores, 4GB RAM - **API Backend**: 4 CPU cores, 8GB RAM - **Database**: 2 CPU cores, 8GB RAM, 100GB SSD - **Cache**: 1 CPU core, 2GB RAM - **Storage**: 500GB cloud storage

**Network Requirements:** - **Internet Bandwidth**: 50-100 Mbps - **Wi-Fi Coverage**: Basic campus coverage - **Concurrent Users**: 200-300 peak

**Estimated Monthly Cost**: $300-600

#### 1.3.1.2 On-Premises Alternative

* **Single Server**: 8 CPU cores, 32GB RAM, 2TB HDD
* **Network Storage**: 5TB NAS
* **UPS**: 1500VA
* **Network**: Managed switch, firewall

**Estimated Hardware Cost**: $15,000-25,000

### 1.3.2 Medium Institution (1,000-5,000 Users)

#### 1.3.2.1 Hybrid Cloud Deployment (Recommended)

**Application Infrastructure:** - **Load Balancer**: 2 CPU cores, 4GB RAM - **Web Applications**: 2x (4 CPU cores, 8GB RAM each) - **API Backend**: 2x (8 CPU cores, 16GB RAM each) - **Database**: Primary + Replica (8 CPU cores, 32GB RAM each) - **Cache Cluster**: 3x (2 CPU cores, 4GB RAM each) - **Storage**: 2TB cloud storage with backup

**Network Requirements:** - **Internet Bandwidth**: 200-500 Mbps with backup - **Wi-Fi Coverage**: Complete campus coverage - **Concurrent Users**: 1,000-1,500 peak

**Estimated Monthly Cost**: $1,200-2,500

#### 1.3.2.2 On-Premises Alternative

* **Application Servers**: 2x (16 CPU cores, 64GB RAM, 1TB SSD)
* **Database Server**: 16 CPU cores, 128GB RAM, 4TB SSD RAID
* **Storage**: 20TB SAN
* **Network**: Enterprise switch, firewall, UPS

**Estimated Hardware Cost**: $60,000-100,000

### 1.3.3 Large Institution (5,000-15,000 Users)

#### 1.3.3.1 Enterprise Cloud Deployment

**Application Infrastructure:** - **Load Balancers**: 2x (4 CPU cores, 8GB RAM each) - **Web Applications**: 4x (8 CPU cores, 16GB RAM each) - **API Backend**: 4x (16 CPU cores, 32GB RAM each) - **Database Cluster**: 3x Primary + 2x Replica (16 CPU cores, 64GB RAM each) - **Cache Cluster**: 6x (4 CPU cores, 8GB RAM each) - **Storage**: 10TB with tiered backup

**Network Requirements:** - **Internet Bandwidth**: 1-2 Gbps with redundancy - **Wi-Fi Coverage**: High-density enterprise coverage - **Concurrent Users**: 3,000-5,000 peak

**Estimated Monthly Cost**: $5,000-10,000

#### 1.3.3.2 On-Premises Alternative

* **Application Tier**: 4x (24 CPU cores, 128GB RAM, 2TB SSD)
* **Database Tier**: 6x (20 CPU cores, 256GB RAM, 8TB SSD RAID)
* **Storage Tier**: 100TB enterprise SAN
* **Network Tier**: Redundant enterprise infrastructure

**Estimated Hardware Cost**: $200,000-400,000

### 1.3.4 Enterprise Institution (> 15,000 Users)

#### 1.3.4.1 Multi-Cloud Enterprise Deployment

**Application Infrastructure:** - **Global Load Balancer**: Multi-region deployment - **Web Applications**: Auto-scaling (8-20 instances) - **API Backend**: Auto-scaling (10-30 instances) - **Database**: Multi-region cluster with read replicas - **Cache**: Distributed cache cluster - **CDN**: Global content delivery network - **Storage**: Distributed storage with global replication

**Network Requirements:** - **Internet Bandwidth**: 5+ Gbps with multiple providers - **Wi-Fi Coverage**: Campus-wide high-density coverage - **Concurrent Users**: 10,000+ peak

**Estimated Monthly Cost**: $15,000-30,000

## 1.4 Network Infrastructure Specifications

### 1.4.1 Internet Connectivity

#### 1.4.1.1 Bandwidth Calculations

* **Base requirement**: 1 Mbps per 50 concurrent users
* **Facial recognition**: Additional 2 Mbps per 100 users
* **Video streaming**: Additional 5 Mbps per 100 users
* **Overhead and redundancy**: 30% additional capacity

#### 1.4.1.2 Connection Types

* **Primary**: Fiber optic (recommended)
* **Backup**: Cable/DSL or cellular
* **Redundancy**: Automatic failover capability

### 1.4.2 Wi-Fi Infrastructure

#### 1.4.2.1 Coverage Requirements

* **Indoor coverage**: 100% building coverage
* **Outdoor coverage**: Key outdoor areas
* **Capacity**: Support for user density
* **Performance**: Minimum 25 Mbps per access point

#### 1.4.2.2 Wi-Fi Standards

* **Minimum**: Wi-Fi 5 (802.11ac)
* **Recommended**: Wi-Fi 6 (802.11ax)
* **Security**: WPA3 Enterprise
* **Management**: Centralized controller

#### 1.4.2.3 Access Point Calculations

* **Indoor**: 1 AP per 2,500 sq ft
* **High-density areas**: 1 AP per 1,000 sq ft
* **Outdoor**: 1 AP per 10,000 sq ft coverage

### 1.4.3 Network Security

#### 1.4.3.1 Firewall Requirements

* **Throughput**: Match internet bandwidth
* **Features**: IPS, content filtering, VPN
* **Redundancy**: High-availability configuration
* **Management**: Centralized security management

#### 1.4.3.2 Network Segmentation

* **DMZ**: Public-facing services
* **Internal**: Private network resources
* **Guest**: Separate guest network
* **IoT**: Isolated IoT device network

## 1.5 Server Hardware Specifications

### 1.5.1 Application Servers

#### 1.5.1.1 Small Deployment

* **CPU**: Intel Xeon or AMD EPYC, 8-16 cores
* **RAM**: 32-64GB DDR4
* **Storage**: 1TB NVMe SSD
* **Network**: Dual 1Gb Ethernet
* **Redundancy**: Single server with backup

#### 1.5.1.2 Medium Deployment

* **CPU**: Intel Xeon or AMD EPYC, 16-32 cores
* **RAM**: 64-128GB DDR4
* **Storage**: 2TB NVMe SSD
* **Network**: Dual 10Gb Ethernet
* **Redundancy**: Load-balanced pair

#### 1.5.1.3 Large Deployment

* **CPU**: Intel Xeon or AMD EPYC, 32-64 cores
* **RAM**: 128-256GB DDR4
* **Storage**: 4TB NVMe SSD RAID
* **Network**: Dual 25Gb Ethernet
* **Redundancy**: Multi-server cluster

### 1.5.2 Database Servers

#### 1.5.2.1 Performance Requirements

* **IOPS**: 10,000+ random IOPS
* **Latency**: < 1ms storage latency
* **Throughput**: 1GB/s+ sequential
* **Reliability**: Enterprise-grade drives

#### 1.5.2.2 Small Database Server

* **CPU**: 8-16 cores, high clock speed
* **RAM**: 64-128GB (large buffer cache)
* **Storage**: 2TB NVMe SSD RAID 1
* **Network**: Dual 10Gb Ethernet

#### 1.5.2.3 Large Database Server

* **CPU**: 32-64 cores, optimized for database
* **RAM**: 256-512GB
* **Storage**: 10TB+ NVMe SSD RAID 10
* **Network**: Dual 25Gb/100Gb Ethernet

### 1.5.3 Storage Systems

#### 1.5.3.1 Network Attached Storage (NAS)

* **Capacity**: 10TB - 100TB
* **Performance**: 10Gb Ethernet connectivity
* **Redundancy**: RAID 6 or RAID 10
* **Backup**: Built-in backup capabilities

#### 1.5.3.2 Storage Area Network (SAN)

* **Capacity**: 50TB - 500TB
* **Performance**: Fibre Channel or iSCSI
* **Redundancy**: Multi-path, redundant controllers
* **Features**: Snapshots, replication, tiering

## 1.6 Software Infrastructure Requirements

### 1.6.1 Operating System Requirements

#### 1.6.1.1 Server Operating Systems

* **Linux**: Ubuntu 20.04 LTS or CentOS 8+ (recommended)
* **Windows**: Windows Server 2019/2022
* **Container**: Docker with Kubernetes orchestration

#### 1.6.1.2 Client Device Requirements

* **Windows**: Windows 10/11
* **macOS**: macOS 10.15+
* **iOS**: iOS 13+
* **Android**: Android 8.0+

### 1.6.2 Database Requirements

#### 1.6.2.1 PostgreSQL Configuration

* **Version**: PostgreSQL 15+
* **Memory**: shared\_buffers = 25% of RAM
* **Storage**: Fast SSD storage
* **Connections**: max\_connections = 500-1000
* **Replication**: Streaming replication for HA

#### 1.6.2.2 Redis Configuration

* **Version**: Redis 7.0+
* **Memory**: 10-20% of total system memory
* **Persistence**: AOF + RDB for durability
* **Clustering**: Redis Cluster for scale

### 1.6.3 Application Stack

#### 1.6.3.1 Backend Requirements

* **Python**: Version 3.9+
* **Django**: Version 4.2+
* **Celery**: For background tasks
* **Gunicorn**: WSGI server
* **Nginx**: Reverse proxy and load balancer

#### 1.6.3.2 Frontend Requirements

* **Node.js**: Version 18+
* **Next.js**: Version 13+
* **TypeScript**: Version 5+
* **Build Tools**: Webpack, Babel

## 1.7 Security Infrastructure

### 1.7.1 Authentication Systems

#### 1.7.1.1 Single Sign-On (SSO)

* **SAML 2.0**: Integration with enterprise SSO
* **OAuth 2.0**: Third-party authentication
* **LDAP/AD**: Directory services integration
* **Multi-factor**: SMS, email, authenticator apps

#### 1.7.1.2 Certificate Management

* **SSL/TLS**: Valid certificates for all endpoints
* **Certificate Authority**: Internal or public CA
* **Auto-renewal**: Automated certificate management
* **Security**: Strong cipher suites only

### 1.7.2 Data Encryption

#### 1.7.2.1 Encryption at Rest

* **Database**: Transparent data encryption
* **Files**: File system encryption
* **Backups**: Encrypted backup storage
* **Keys**: Hardware security modules (HSM)

#### 1.7.2.2 Encryption in Transit

* **HTTPS**: All web traffic encrypted
* **API**: All API calls encrypted
* **Database**: Encrypted database connections
* **Internal**: Inter-service encryption

## 1.8 Monitoring and Logging

### 1.8.1 System Monitoring

#### 1.8.1.1 Infrastructure Monitoring

* **Servers**: CPU, memory, disk, network metrics
* **Applications**: Response times, error rates
* **Database**: Query performance, connection pools
* **Network**: Bandwidth utilization, latency

#### 1.8.1.2 Application Monitoring

* **User Experience**: Page load times, availability
* **Business Metrics**: User activity, feature usage
* **Security**: Failed logins, suspicious activity
* **Performance**: API response times, throughput

### 1.8.2 Log Management

#### 1.8.2.1 Log Collection

* **Application Logs**: Structured JSON logging
* **System Logs**: OS and service logs
* **Security Logs**: Authentication and access logs
* **Audit Logs**: All system changes tracked

#### 1.8.2.2 Log Analysis

* **Centralized**: ELK stack or similar
* **Real-time**: Stream processing
* **Alerting**: Automated alert generation
* **Retention**: Compliance-based retention

## 1.9 Backup and Disaster Recovery

### 1.9.1 Backup Strategy

#### 1.9.1.1 Data Backup

* **Database**: Continuous backup with point-in-time recovery
* **Files**: Daily incremental, weekly full backups
* **Configuration**: Version-controlled configuration
* **Testing**: Regular backup restore testing

#### 1.9.1.2 Backup Infrastructure

* **Local**: On-site backup for quick recovery
* **Offsite**: Cloud or remote backup storage
* **Encryption**: All backups encrypted
* **Automation**: Fully automated backup processes

### 1.9.2 Disaster Recovery

#### 1.9.2.1 Recovery Objectives

* **RTO**: Recovery Time Objective (2-8 hours)
* **RPO**: Recovery Point Objective (15 minutes - 1 hour)
* **Testing**: Quarterly DR testing
* **Documentation**: Detailed recovery procedures

#### 1.9.2.2 DR Infrastructure

* **Hot Standby**: Real-time replication
* **Warm Standby**: Near real-time replication
* **Cold Standby**: Periodic backup restoration
* **Geographic**: Geographically separated DR site

## 1.10 Performance Optimization

### 1.10.1 Database Optimization

#### 1.10.1.1 Query Performance

* **Indexing**: Proper database indexing
* **Query Analysis**: Regular query performance review
* **Connection Pooling**: Efficient connection management
* **Caching**: Query result caching

#### 1.10.1.2 Scaling Strategies

* **Read Replicas**: Scale read operations
* **Partitioning**: Table and database partitioning
* **Sharding**: Horizontal database scaling
* **Clustering**: Database cluster deployment

### 1.10.2 Application Optimization

#### 1.10.2.1 Code Optimization

* **Profiling**: Regular application profiling
* **Caching**: Multi-level caching strategy
* **Async Processing**: Background task processing
* **Resource Management**: Efficient resource usage

#### 1.10.2.2 Scaling Strategies

* **Horizontal Scaling**: Multiple application instances
* **Load Balancing**: Traffic distribution
* **Auto-scaling**: Dynamic scaling based on load
* **CDN**: Content delivery network usage

## 1.11 Compliance and Audit Requirements

### 1.11.1 Data Protection Compliance

#### 1.11.1.1 GDPR Compliance

* **Data Mapping**: Complete data inventory
* **Consent Management**: User consent tracking
* **Access Rights**: Data subject access rights
* **Breach Notification**: Automated breach detection

#### 1.11.1.2 Educational Privacy

* **FERPA**: Student record protection
* **Local Laws**: Regional privacy requirements
* **Data Retention**: Compliant data retention
* **Audit Trails**: Complete audit logging

### 1.11.2 Security Compliance

#### 1.11.2.1 Security Standards

* **ISO 27001**: Information security management
* **SOC 2**: Service organization controls
* **NIST**: Cybersecurity framework
* **Industry**: Education-specific standards

#### 1.11.2.2 Audit Requirements

* **Access Logs**: Complete access logging
* **Change Management**: All changes tracked
* **Configuration**: Baseline configurations
* **Vulnerability**: Regular security assessments

## 1.12 Implementation Timeline

### 1.12.1 Phase 1: Infrastructure Setup (Weeks 1-4)

* Network infrastructure deployment
* Server hardware installation
* Basic software installation
* Security configuration

### 1.12.2 Phase 2: Application Deployment (Weeks 5-8)

* Application server configuration
* Database setup and optimization
* Load balancer configuration
* Initial testing

### 1.12.3 Phase 3: Integration and Testing (Weeks 9-12)

* System integration
* Performance testing
* Security testing
* User acceptance testing

### 1.12.4 Phase 4: Go-Live Preparation (Weeks 13-16)

* Final configurations
* Data migration
* Staff training
* Go-live execution

## 1.13 Cost Estimates by Component

### 1.13.1 Hardware Costs

| Scale | Servers | Storage | Network | Total Hardware |
| --- | --- | --- | --- | --- |
| Small | $15,000 | $5,000 | $8,000 | $28,000 |
| Medium | $60,000 | $20,000 | $25,000 | $105,000 |
| Large | $200,000 | $75,000 | $60,000 | $335,000 |
| Enterprise | $500,000 | $200,000 | $150,000 | $850,000 |

### 1.13.2 Software Costs (Annual)

| Scale | OS/DB | Security | Monitoring | Total Software |
| --- | --- | --- | --- | --- |
| Small | $5,000 | $3,000 | $2,000 | $10,000 |
| Medium | $15,000 | $10,000 | $8,000 | $33,000 |
| Large | $40,000 | $25,000 | $20,000 | $85,000 |
| Enterprise | $100,000 | $60,000 | $50,000 | $210,000 |

### 1.13.3 Support and Maintenance (Annual)

| Scale | Hardware | Software | Total Support |
| --- | --- | --- | --- |
| Small | $3,000 | $2,000 | $5,000 |
| Medium | $10,000 | $7,000 | $17,000 |
| Large | $35,000 | $18,000 | $53,000 |
| Enterprise | $85,000 | $42,000 | $127,000 |

## 1.14 Conclusion

The technical architecture and infrastructure requirements for the Signox LogX System scale significantly based on institution size and complexity. Proper planning and implementation of the infrastructure components outlined in this document are critical for system success.

### 1.14.1 Key Recommendations

1. **Start with Scalable Architecture**: Design for growth from the beginning
2. **Prioritize Security**: Implement comprehensive security measures
3. **Plan for Monitoring**: Include monitoring and logging from day one
4. **Consider Cloud Options**: Evaluate cloud vs. on-premises carefully
5. **Test Thoroughly**: Comprehensive testing before go-live

### 1.14.2 Next Steps

1. Complete the Client Requirements Form
2. Conduct technical assessment of current infrastructure
3. Develop detailed implementation plan
4. Procure necessary hardware and software
5. Begin phased implementation

**Document Version:** 1.0  
**Last Updated:** June 2025  
**Document Owner:** Signox LogX Technical Team